Journal of Universal Computer Science, vol. 30, no. 9 (2024), 1265-1283
submitted: 27/9/2023, accepted: 30/5/2024, appeared: 14/9/2024

Recognition of genuine and phishing emails may not be associated with response to phishing attacks

Alex Crgol
(University of Maribor, Maribor, Slovenia, alex.crgol@student.um.si)

Simon Vrhovec
(University of Maribor, Maribor, Slovenia
https://orcid.org/0000-0002-6951-6369, simon.vrhovec@um.si)

Abstract: This paper investigates the associations between recognition of phishing and genuine emails, and response to phishing attacks, namely susceptibility to phishing emails (i.e., click rate) and full phishing attack compliance (i.e., click on a malicious link followed by an attempt to download a file). A cross-sectional survey was conducted among students at a Slovenian university ($N = 135$) to assess how participants recognize examples of phishing emails. Additionally, a field trial study (i.e., a phishing campaign) was performed to test participants' response to a real phishing attack. Chi-square and Fisher's exact tests were used to test the hypothesized associations between the studied constructs. Results do not indicate any significant associations between recognition of neither phishing nor genuine emails and response to phishing attacks. These findings suggest that studies should thus avoid using recognition of genuine and/or phishing emails in their research designs despite its convenience since it has little practical merit. These results also seriously undermine the assumptions that current phishing training is built on. The focus of phishing training may thus switch from knowledge-raising to actual response to phishing attacks, for example, through practical phishing attempts at the workplace. Although this is not a new phishing training approach, it may have some unwanted side-effects which future studies could focus on tackling.

Keywords: Information security, cybersecurity, cyber attack, cyber threat, organization vulnerability, targeted phishing, spear phishing, context-aware phishing
Categories: H.1.2, J.1, K.4.4, K.6.5
DOI: 10.3897/jucs.132113

1 Introduction

Phishing remains one of the major problems in providing cybersecurity to individuals and organizations alike [Zheng et al., 2022, Mughaid et al., 2022]. Phishing is an attack in which an attacker impersonates a trusted entity in order to convince a victim to perform a malicious act, such as providing personal information, clicking on a malicious link or opening a malicious attachment [Das et al., 2020, Mihelič et al., 2019]. Phishing attacks on organizations employ a variety of techniques that take advantage of both technological and behavioral weaknesses [Butavicius et al., 2022]. In order to trick email recipients into clicking on harmful links or giving out sensitive information, phishing attempts frequently utilize false emails that appear to be from reliable sources, such as banks or reputable organizations [Alabdan, 2020]. These emails are carefully crafted to appear genuine often using social engineering techniques to manipulate individuals into taking action [Gordon et al., 2019]. One of the reasons phishing is a common vector of cyber threats is its ability to exploit human weaknesses and manipulate individuals

into divulging sensitive information [Lain et al., 2022]. Employees therefore pose a serious cybersecurity risk for organizations due to their vulnerability to phishing emails [Bayl-Smith et al., 2022]. Factors, such as high employee turnover, lack of cybersecurity training, and the constant influx of new employees may additionally contribute to the vulnerability of organizations to phishing attacks [Iuga et al., 2016]. Furthermore, phishing emails can be realistic and convincingly spoof the identity of trusted individuals or organizations making it difficult for email recipients to discern their malicious intent [Gordon et al., 2019]. The success of phishing attacks also relies on the lack of awareness and knowledge about phishing techniques among individuals [Diaz et al., 2020]. Studies indicate that susceptibility to phishing can be influenced by factors, such as cyber training, anxiety, stress, risk-taking, involvement in cyber clubs or scholarship programs, college affiliation, academic year progression, fear of COVID-19, age and gender [Diaz et al., 2020, Yoro et al., 2023, Abroshan et al., 2021, Sutter et al., 2022]. Lack of awareness and understanding of phishing characteristics can also lead to higher susceptibility to these attacks [Lee et al., 2023]. To mitigate the risks of phishing attacks, organizations can implement measures such as employee education and awareness programs, robust cybersecurity policies, and the use of advanced detection technologies [Sharma et al., 2022]. Training employees to recognize phishing emails, encouraging them to report suspicious emails, and implementing multi-factor authentication can help strengthen an organization's defense against phishing attacks [Lappas and Karampelas, 2023]. Additionally, ongoing research and development of anti-phishing software and algorithms are crucial in detecting and preventing phishing attacks [Tultul et al., 2022]. Nevertheless, they are not perfect and it is therefore still people who ultimately receive phishing emails and need to adequately respond to them [Mihelič et al., 2019].

Studying phishing is essential for addressing these challenges which have not been yet adequately addressed as seen by recent cybersecurity reports [SI-CERT, 2023, CERT-EU, 2024]. A stream of phishing studies focuses on the actual response to phishing attacks. For example, [Bayl-Smith et al., 2022] studied response to phishing attacks as the dependent variable for their research model based on the protection motivation theory. [Diaz et al., 2020], [Hassandoust et al., 2020] and [Yoro et al., 2023] studied factors associated with actual response to phishing attacks. [Gordon et al., 2019] report on a retrospective study of simulated phishing attacks in health care institutions. [Sutter et al., 2022] investigated the impact of different phishing training approaches on the response of participants. [Lain et al., 2022] conducted a large-scale and long-term study of phishing attacks in an organization. They found, for example, that phishing training commonly found in organizations today can have the adverse effect of increasing phishing susceptibility. Another stream of studies focus on the recognition of phishing emails. For example, [Nasser et al., 2020] studied the role of cue utilization and cognitive load in recognition of phishing emails. [Iuga et al., 2016] aimed to identify factors related to individuals' susceptibility to phishing attacks although focusing on recognition of phishing websites. [Abroshan et al., 2021] studied various factors, including those related to the COVID-19 pandemic, associated with success of phishing attacks during the pandemic albeit focusing on the recognition of phishing emails. [Parsons et al., 2017] associate the results of an empirical lab-based phishing experiment (i.e., recognition of phishing emails) with an aspect of information security behavior. It may be worthwhile to note that some of these studies assume that an individual's ability to recognize phishing emails is either associated with, an indicator of secure behavior or some aspect thereof.

The association between recognition of phishing emails and response to phishing attacks (i.e., an example of secure behavior) is however rarely studied. The scarcity of studies on the relation between recognition of phishing emails and actual response to

phishing attacks could be a consequence of the inability to obtain results that would establish a definite relation between knowledge (e.g., ability to recognize phishing emails) and behavior (e.g., response to a phishing attack). This would be in line with the common belief in the cybersecurity community that self-reported behavior and actual behavior may significantly differ. Although they are very few, some studies examine both recognition of phishing emails and the actual response to phishing. For example, [Williams et al., 2023] studied the role of conscientiousness and cue utilization in both recognition of phishing emails and response to phishing attacks among students. Although the study found differing roles of the studied factors between both settings, it did not attempt to relate phishing recognition and response to phishing attacks. This paper aims to fill in the presented gap by purposely aiming to determine whether an association between recognition of phishing emails and response to phishing attacks exists.

The paper is structured as follows. In Section 4, we provide details on the research method employed. We present the results in Section 5. We discuss the findings of the reported study, its limitations and provide directions for future work in Section 6.

2 Theoretical background

A phishing attack is a type of a social engineering attack in which an attacker seeks to obtain a victim's personal information or compromise their devices [Andress, 2019]. To achieve this, the victim must be persuaded to share private information, such as credentials, or click on a malicious link in a phishing email [Alkhalil et al., 2021]. Fake websites, also referred to as phishing or landing websites, are often coupled with phishing emails and closely resemble real websites, such as those of banks, social media sites, or real businesses [Alawida et al., 2022]. Traditional blanket (mass) phishing attacks, and targeted or spear phishing attacks are currently the best-known and frequent phishing phenomenon [Adebowale, 2021, Mihelič et al., 2019].

Blanket phishing, also known as mass phishing and in some cases spam, leans on the sheer volume of messages sent, basic deception techniques and impersonation of the sender and the use of an opportunistic strategy [Heartfield and Loukas, 2016, Parmar, 2012, Mihelič et al., 2019]. There is some confusion surrounding the relation between spam and mass phishing. While spam can be considered as advertisement, it may lack the social engineering component which is characteristic of all phishing types [Das et al., 2020]. Prospective victims can typically tell whether an email or website is fraudulent because of its poor language and obviously incorrect domain names [Alanezi, 2021]. Typically, traditional email phishing attacks are sent in bulk to hundreds or thousands of email recipients. The success rate of these attacks might vary significantly based on the message quality [Bullee et al., 2017]. Nevertheless, even a very low success rate results in some success due to the number of attacked individuals.

Spear phishing, also known as targeted or context-aware phishing, is a targeted attack against particular targets, such as an individual and his associates or an organization [Ghazi-Tehrani and Pontell, 2021, Heartfield and Loukas, 2016]. Messages are better planned and tailored to a specific situation, for example, sending an email related to a targeted department. Attackers can invest considerable amounts of time to learn about their targets by acquiring vast amounts of data and information about the targeted individual or organization and their likely contacts [Das et al., 2020]. In order to deceive the email recipient into providing their credentials or installing malware to their devices, attackers utilize the acquired information to make the attack appear as genuine as possible [Ghazi-Tehrani and Pontell, 2021, Mihelič et al., 2019]. Attackers often send emails that

appear and seem authentic and trustworthy which includes customary logos, images, and signatures. Even harmful links and attachments in phishing emails may be concealed or made seem genuine [Hassandoust et al., 2020]. Users typically find it more challenging to notice and defend against this sort of attacks because of the highly sophisticated content and well-planned graphic form of phishing emails [Jampen et al., 2020]. The most sophisticated spear phishing attacks, sometimes referred to as spear phishing – APT (*advanced persistent threat*), have a high degree of contextual awareness, personalization and proper timing, and can succeed unnoticed by the targets [Mihelič et al., 2019]. Such attacks are however much less frequent than the everyday targeted phishing attacks we have become more or less used to.

3 Hypotheses development

In this study, we focus on targeted phishing attacks which are common today [ENISA, 2023, CERT-EU, 2024]. Since training is considered as a key strategy for dealing with the human aspect of phishing attacks (i.e., susceptibility) [Lappas and Karampelas, 2023, Iuga et al., 2016, Diaz et al., 2020, Sutter et al., 2022], we can assume that the ability to recognize phishing emails gained in phishing training relates to individuals' response to phishing attacks albeit we could not find any definitive evidence about this in the literature. Similarly, we can assume that the ability to recognize genuine emails is also related to individuals' response to phishing attacks since it may indicate their ability to discern genuine from phishing emails.

Individuals can respond to phishing attacks in several ways. First, an individual might not see the phishing email, for example, due to technical protection mechanisms, such as spam filters. Second, an individual may see but ignore a phishing email. Such response may be quite common due to the pervasiveness of attempted phishing emails today. This can also be a consequence of technical mechanisms for marking email as spam (e.g., in the subject). Third, phishing emails employ various strategies for tricking individuals into doing some malicious actions. Typically, an individual may click on a malicious link or open a malicious attachment in a phishing email. We can consider a phishing attack as successful as soon as it prompts individuals to do any of these malicious actions. Although clicking on a malicious link or opening a malicious attachment can be the final step in a phishing attack that enables the attackers to achieve their goals (e.g., infection with malware, drive-by downloads), phishing attacks may involve further steps. Fourth, assuming that the phishing attack involves further steps, individuals may follow attackers' instructions, for example, on a landing phishing website, such as providing personal information or clicking on further links. We can consider that individuals complied with the phishing attack in such cases. It may be worthy to note that such further compliance with attackers' instructions is not required for a phishing attack to succeed since a device may be already compromised in the previous step. Fifth, individuals may report the phishing attack to an adequate reporting point. Such reports may help organizations identify broader phishing campaigns early and timely tackle them [Mihelič et al., 2019].

Based on the above, we pose the following sets of hypotheses:

H1a: Ability to recognize phishing emails is associated with susceptibility to phishing emails.

H1b: Ability to recognize genuine emails is associated with susceptibility to phishing emails.

H2a: Ability to recognize phishing emails is associated with full phishing attack compliance.

H2b: Ability to recognize genuine emails is associated with full phishing attack compliance.

4 Methods

4.1 Research design

This study employed a cross-sectional survey design for assessing how participants recognize phishing and genuine emails. The test included eight different emails (four phishing and four genuine) out of which two phishing and two genuine emails were selected for each participant. Afterwards, we conducted a field trial study (i.e., a phishing campaign) to test participants' response to a real phishing attack. We observed whether participants did not respond to the phishing email, clicked on a link in the phishing email, wanted to download a file from the phishing (landing) website and/or reported the phishing email. This enabled us to determine whether the results of phishing emails recognition were associated with response to a real phishing attack.

4.2 Ethical considerations

The study proposal was approved on 28 February 2022 by the Research Ethics Committee of the University of Maribor, Faculty of Criminal Justice and Security.

4.3 Measures

Theoretical constructs were defined and operationalized as presented in Table 1.

Theoretical construct	Operational definition
Recognition of genuine email	An individual's ability to recognize a genuine email as such.
Recognition of phishing email	An individual's ability to recognize a phishing email as such.
Susceptibility to phishing emails	An individual's susceptibility to clicking on a link in a phishing email (i.e., clicking on a link regardless of further actions taken).
Full phishing attack compliance	An individual's compliance with all instructions in a phishing attack (i.e., clicking on a link followed by an attempt to download a file).

Table 1: Definitions of theoretical constructs.

Emails used in the recognition survey were real-world examples of phishing and non-phishing emails. Emails were adapted for this study by replacing any personal information with generic information (e.g., using a generic name and email address). All eight emails are presented in Appendix A. The topics covered the major attacking styles targeting some of the most common targets, including bank users, users of postal services and users of virtual meeting platforms [SI-CERT, 2023, SlashNext, 2023]. Recognition of phishing and non-phishing emails was measured by respondents indicating whether they believed an email was phishing (response *Phishing*) or not (response *Genuine*).

Respondents could also indicate that they were unsure whether an email was phishing or genuine (response *Don't know*).

A phishing email and landing phishing website on the topic of COVID-19 were developed for this study. Responses to phishing emails were monitored through a remote email and web server. After the phishing campaign started, the server monitored the actions taken by the participants. First, phishing emails were sent by the server (*email sent*). The phishing email is shown in Figure 1.

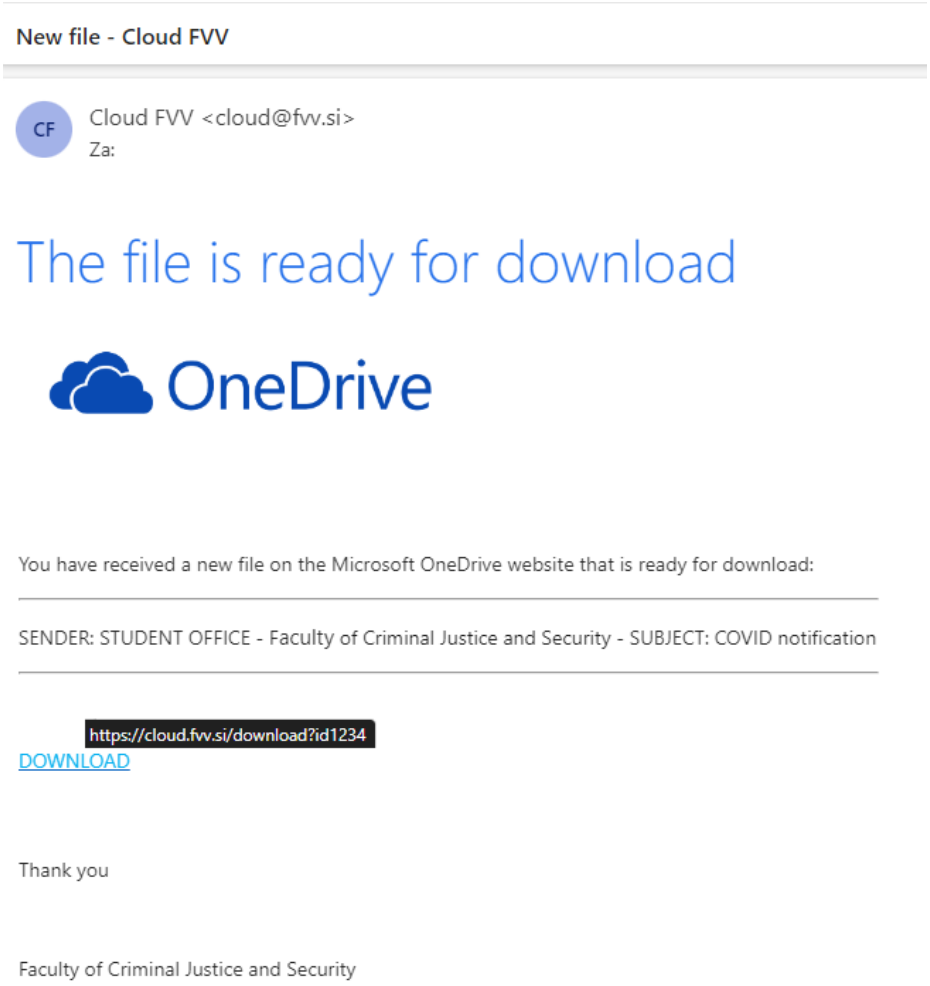

Figure 1: Phishing email.

Second, phishing emails had remote images integrated which enabled us to monitor whether participants opened the sent emails (*email opened*). This status is however

unreliable since certain email clients and/or their security and privacy-preserving settings block such type of remote monitoring. Third, the phishing email included a link to the landing phishing website hosted by the server which enabled us to monitor whether participants clicked on the link (*clicked link*). The landing phishing website is presented in Figure 2.

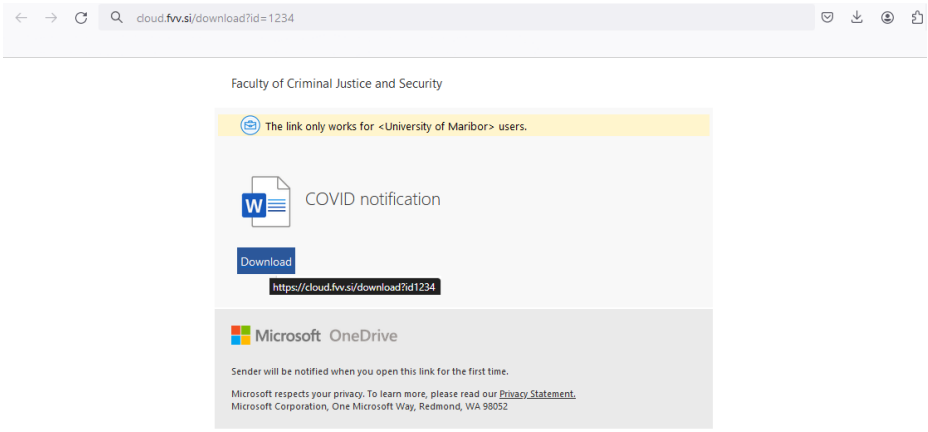

Figure 2: Landing phishing website.

Fourth, the landing phishing website included a button that appeared to download a document but only included a link to a monitored URL. This enabled us to monitor whether participants intended to download the file (*download file*). Fifth, we informed in advance the key points the students were likely to report the phishing attempt to (i.e., the national CERT, the university IT Department, the Student Office, IT Department and Secretary of the faculty). Although we could monitor whether participants reported the phishing attack at predicted reporting points internally (*reported*), the national CERT was not allowed to provide us with any feedback. Additionally, we did not inform all faculty and university employees about the phishing campaign in order not to compromise it. Consequentially, some reports may have gone unnoticed thus considerably lowering the reliability of this measure.

4.4 Sample and data collection

An invitation to complete the survey was sent to 483 students of University of Maribor, Faculty of Criminal Justice and Security. The invitation was sent by the Student Office and included a statement of support by the Student Council. The survey was conducted from 28 March 2022 to 18 April 2022. We received a total of $N = 135$ useful responses. The survey was pseudo anonymous since this was essential to match the results of the survey to the results of the phishing campaign. Characteristics of the sample are presented in Table 2. The age of respondents ranged from 18 to 57 years old ($M = 24.6, SD = 7.2$). The sample includes both part and full time students. The former are typically older than full time students.

All respondents were included in the phishing campaign. The phishing campaign was launched on 10 May 2022 and was monitored until 17 May 2022. Out of 135 sent phishing

Characteristic		Frequency	Percent
Gender	Female	86	63.7
	Male	48	35.6
	N/A	1	0.7
Living environment	A house in the countryside	3	2.2
	Settlement	12	8.9
	Village	48	35.6
	Smaller town	19	14.1
	Major city	53	39.3
Primary source of information	Printed media	0	0.0
	Radio	1	0.7
	TV	7	5.2
	Internet	123	91.1
	Family and friends	4	3.0

Table 2: Sample characteristics.

emails, 64 participants (47.4 percent) fully complied with the phishing attack (i.e., clicked the phishing link and attempted to download a file from the landing phishing website). Additional 10 participants (7.4 percent) were proven to be susceptible to the phishing attack (i.e., clicked the phishing link without attempting to download the file). Out of the remaining 61 participants (45.2 percent), 25 (18.5 percent) opened the email without clicking the phishing link. For the remaining 36 participants (26.7 percent), we are unsure whether they saw the email or not. A total of five participants (3.7 percent) reported the phishing attack. Four participants (3.0 percent) reported the attack to the Student Office and one participant (0.7 percent) to the faculty IT Department. The participant who reported the attack to the faculty IT Department did not appear to have seen the email as their email client did not load remote content. Three participants who reported the phishing attack to the Student Office fully complied with the phishing attack, and one participant reported the phishing attack without clicking on the phishing link.

4.5 Data analysis

We tested the associations between the respondents' ability to recognize phishing/genuine emails and their response to phishing attacks for each email separately. This enabled us to determine whether the type of phishing/genuine emails affects these associations. Prior to the analysis, we re-coded responses for recognition of phishing and non-phishing emails. If a respondent guessed correctly whether an email was phishing or genuine, their answer was re-coded to *Yes* otherwise it was re-coded to *No* which always included responses *Don't know*.

We employed both the *chi-square test of independence* and *Fisher's exact test* to determine the range of significance for the hypothesized associations. Fisher's exact test was employed since the number of rows and columns was fixed by the study design (2×2). While the chi-square test if often used to test associations between two categorical variables, we wanted to gain more insights into the statistical significance of the tested associations. The most commonly used significance level is $\alpha = 0.05$ meaning p-values below this threshold indicate statistical significance. The two other often used significance levels are $\alpha = 0.01$ and $\alpha = 0.001$. In rare cases, a significance level of $\alpha = 0.1$ can also be acceptable. Fisher's exact test is considered as more conservative than the chi-square test since its p-values are larger than p-values obtained from chi-square tests. Additionally, Fisher's exact test is an alternative way to determine the significance of an association if more than 20 percent of cells in the frequency table have expected cell

counts of less than 5. We report all test results according to APA requirements. Data was analyzed with IBM SPSS Statistics version 28.

5 Results

Table 3 shows frequencies for phishing emails. Chi-square tests of independence showed that there was no significant association between susceptibility to phishing emails and recognition of phishing emails (Accounting $\chi^2(1, N = 71) = 0.486, p = 0.486$, Post of Slovenia $\chi^2(1, N = 64) = 0.271, p = 0.603$, Google $\chi^2(1, N = 71) = 0.058, p = 0.810$, Zoom $\chi^2(1, N = 64) = 2.222, p = 0.136$). Fisher's exact tests also did not indicate a significant association between susceptibility to phishing emails and recognition of phishing emails (Accounting $p = 0.622$, Post of Slovenia $p = 0.752$, Google $p = 1.000$, Zoom $p = 0.193$). Therefore, these results do not provide any support for hypothesis H1a (all $p > 0.1$).

Email			Susceptibility No	Susceptibility Yes	Full compliance No	Full compliance Yes	Total
Accounting	Recognition	No	10	17	12	15	27
		Yes	20	24	21	23	44
		Total	30	41	33	38	71
Post of Slovenia	Recognition	No	5	7	6	6	12
		Yes	26	26	32	20	52
		Total	31	33	38	26	64
Google	Recognition	No	8	12	8	12	20
		Yes	22	29	25	26	51
		Total	30	41	33	38	71
Zoom	Recognition	No	14	9	15	8	23
		Yes	17	24	23	18	41
		Total	31	33	38	26	64

Table 3: Frequency tables for phishing emails.

Chi-square tests of independence showed that there was no significant association between full phishing attack compliance and recognition of phishing emails (Accounting $\chi^2(1, N = 71) = 0.072, p = 0.788$, Google $\chi^2(1, N = 71) = 0.470, p = 0.493$, Zoom $\chi^2(1, N = 64) = 0.508, p = 0.476$). The results of the chi-square test for Post of Slovenia ($\chi^2(1, N = 64) = 0.538, p = 0.463$) were not reliable since one cell (25 percent of cells) had expected count of less than 5 (the minimum expected count was 4.88). Fisher's exact tests additionally did not indicate a significant association between susceptibility to phishing emails and recognition of phishing emails (Accounting $p = 0.811$, Post of Slovenia $p = 0.525$, Google $p = 0.600$, Zoom $p = 0.598$). These results thus do not provide any support for hypothesis H2a (all $p > 0.1$).

Table 4 shows frequencies for genuine emails. Chi-square tests of independence showed that there was no significant association between susceptibility to phishing emails and recognition of genuine emails (Student service $\chi^2(1, N = 64) = 0.018, p = 0.895$, WeTransfer $\chi^2(1, N = 71) = 1.253, p = 0.263$, Apple Inc. $\chi^2(1, N = 64) = 2.541, p = 0.111$, Intesa Sanpaolo Bank $\chi^2(1, N = 71) = 0.053, p = 0.817$). Fisher's exact tests also did not indicate a significant association between susceptibility to phishing emails and recognition of genuine emails (Student service $p = 1.000$, WeTransfer $p = 0.301$, Apple Inc. $p = 0.131$, Intesa Sanpaolo Bank $p = 1.000$). Thus, these results do not provide any support for hypothesis H1b (all $p > 0.1$).

Email			Susceptibility No	Susceptibility Yes	Full compliance No	Full compliance Yes	Total
Student service	Recognition	No	7	7	8	6	14
		Yes	24	26	30	20	50
		Total	31	33	38	26	64
WeTransfer	Recognition	No	19	31	22	28	50
		Yes	11	10	11	10	21
		Total	30	41	33	38	71
Apple Inc.	Recognition	No	9	16	12	13	25
		Yes	22	17	26	13	39
		Total	31	33	38	26	64
Intesa Sanpaolo Bank	Recognition	No	16	23	18	21	39
		Yes	14	18	15	17	32
		Total	30	41	33	38	71

Table 4: Frequency tables for genuine emails.

Chi-square tests of independence showed that there was no significant association between full phishing attack compliance and recognition of genuine emails (Student service $\chi^2(1, N = 64) = 0.037, p = 0.847$, WeTransfer $\chi^2(1, N = 71) = 0.418, p = 0.518$, Apple Inc. $\chi^2(1, N = 64) = 2.201, p = 0.138$, Intesa Sanpaolo Bank $\chi^2(1, N = 71) = 0.004, p = 0.952$). Fisher's exact tests also did not indicate a significant association between susceptibility to phishing emails and recognition of genuine emails (Student service $p = 1.000$, WeTransfer $p = 0.606$, Apple Inc. $p = 0.193$, Intesa Sanpaolo Bank $p = 1.000$). These results therefore do not provide any support for hypothesis H2b (all $p > 0.1$).

6 Discussion

This study investigated the associations between recognition of genuine and phishing emails, and response to phishing attacks, namely susceptibility to phishing emails (i.e., click rate) and full phishing attack compliance (i.e., click on a malicious link followed by an attempt to download a file). Even though no significant associations were detected in this study indicating no support for the posed hypotheses, this paper makes two key contributions to the literature and outlines some recommendations for future studies.

First, we tested both recognition of genuine and phishing emails and found no significant associations between recognition and neither susceptibility to phishing emails nor full phishing attack compliance contributing to the literature on phishing attacks. Both genuine and phishing emails included in our study proved to have varying levels of difficulty. Successful phishing email recognition ranged from 62.0 percent (Accounting) to 81.3 percent (Post of Slovenia), and successful genuine email recognition ranged from 29.6 percent (WeTransfer) to 78.1 percent (Student service). These results suggest that recognition difficulty level may not be a factor in response to actual phishing attacks. Future studies should thus avoid using recognition of genuine and/or phishing emails in their research designs despite its convenience since it has little practical merit. Actual response to phishing attacks may be measured instead. There is however a barrier to conducting such studies in real organizations due to potentially endangering participating individuals and/or organizations. Since it may be exceedingly difficult to obtain non-student samples in the cybersecurity area, student samples may be disproportionately valuable in phishing studies.

Next, the results of our study have implications for phishing training as well. Since there was no association between the ability to recognize phishing emails and response to

actual phishing emails, these results seriously undermine the assumptions that phishing training is built on. This aligns well with the literature that questions the efficacy of phishing training [Lain et al., 2022]. Phishing training may thus need to be conceptually adapted to focus on actual phishing attacks instead of raising awareness, knowledge and the ability to recognize phishing attacks. Therefore, the focus of phishing training may switch from knowledge-raising as its with most current phishing and security training [Patil and Arra, 2022, Fujs et al., 2020] to actual response to phishing attacks, for example, through practical phishing attempts at the workplace. This is not a new approach to phishing training. However, attacking employees of an organization can have some unwanted side-effects, such as increased mistrust between the security and other departments or reluctance to answer all emails. Future work may thus aim to facilitate such practical phishing drills and perhaps routinize them similarly to how fire drills are regularly performed on boats. Future studies may also pursue other directions for improving the current phishing training approaches, such as tailoring phishing training to individuals. For example, phishing training may be adapted to an individual's existing knowledge, attitude and behavior [Fujs et al., 2021]. Since purely individualized training may be costly [Fujs et al., 2022], especially in large organizations, such training approaches could leverage artificial intelligence for automation of the tailoring process (e.g., according to an individual's phishing training and response history).

There are some limitations that the readers should note. First, we could not ascertain that all respondents actually saw the phishing emails. Although we could monitor whether an embedded image loaded in a participant's email client, some clients block loading of such remote content. We therefore assumed that all recipients saw the phishing email during the phishing campaign monitoring period. Also, we could not reliably measure reporting of the phishing attack. Next, we used a single phishing email in the phishing campaign. Future studies with a wider variety of emails used in the phishing campaign would be needed to further confirm the results of this study. Significantly larger samples would be required to avoid attacking participants with several phishing emails. Further, we did not study the reasons for participants clicking and/or following instructions. Individuals may have recognized attempted phishing attacks but nevertheless clicked and/or proceeded to fully comply with attackers' instructions to investigate them regardless of the risk of taking such a course of action. However, organizations may have inadequate practices for investigating phishing attacks which could expose their systems further [Mihelič et al., 2019]. As with organizations, not all individuals who investigate such phishing attacks have the expertise needed to protect their devices from being compromised by a malicious phishing attack. Future studies may investigate the association between ability and reasons to conduct such investigations. Next, the study was done at a single university in a single cultural context. Future studies in different settings, such as various universities, other organizations and countries may be highly beneficial. Finally, future studies with larger samples and a wider variety of emails used for measuring recognition of phishing and genuine emails would be beneficial for further confirming the results of this study.

A Emails used for assessing how participants recognize phishing and genuine emails

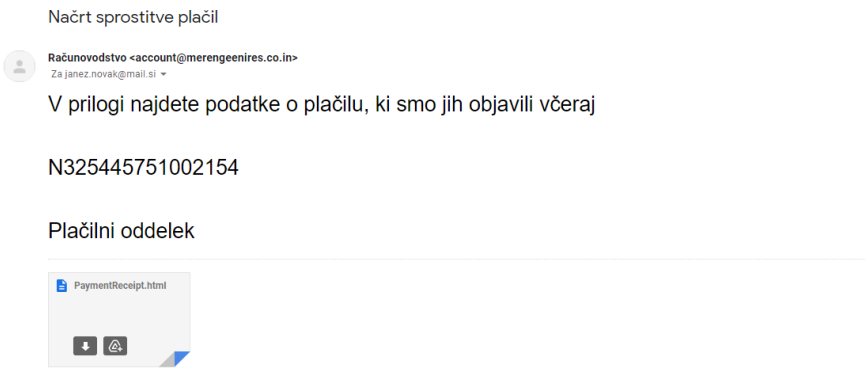

Figure 3: Accounting (phishing).

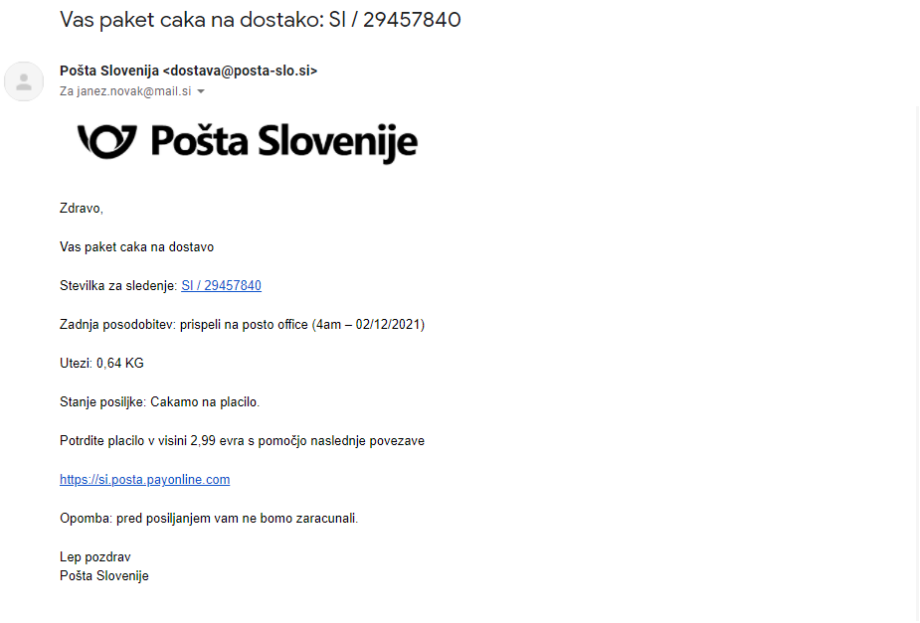

Figure 4: Post of Slovenia (phishing).

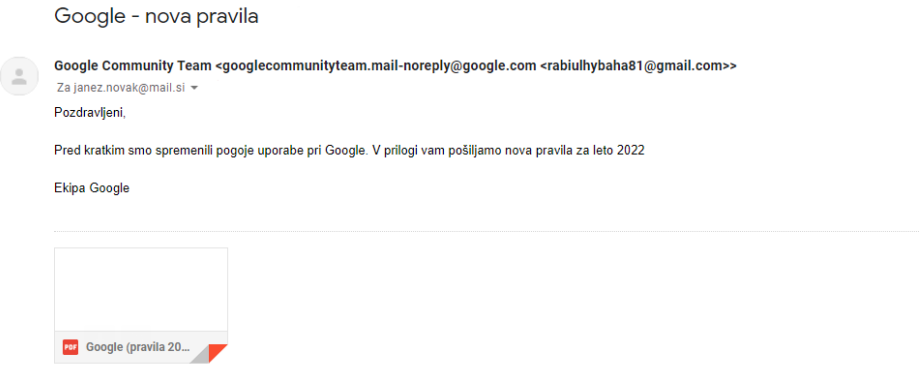

Figure 5: Google (phishing).

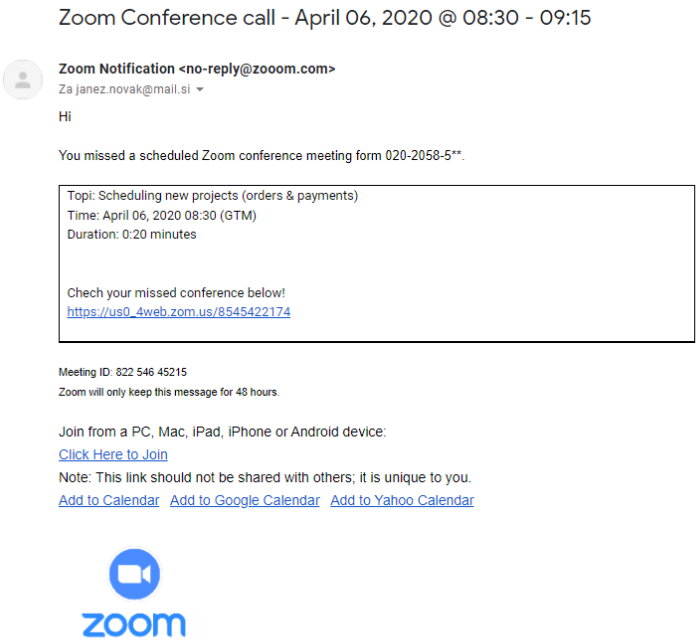

Figure 6: Zoom (phishing).

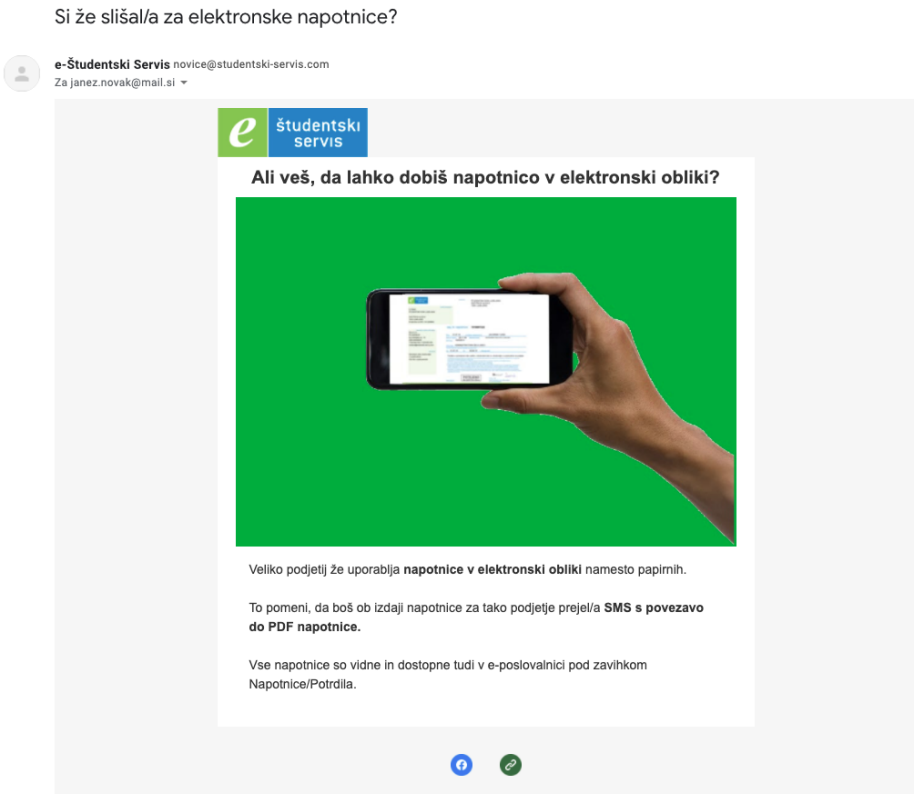

Figure 7: Student service (genuine).

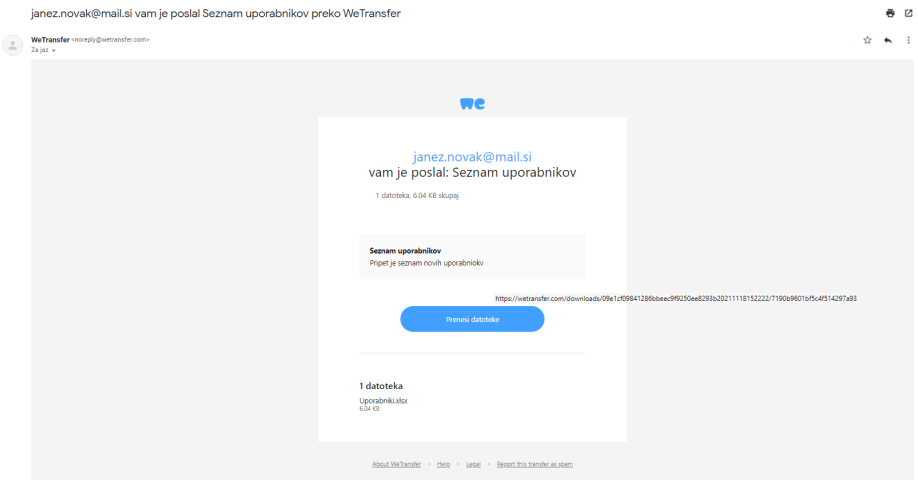

Figure 8: WeTransfer (genuine).

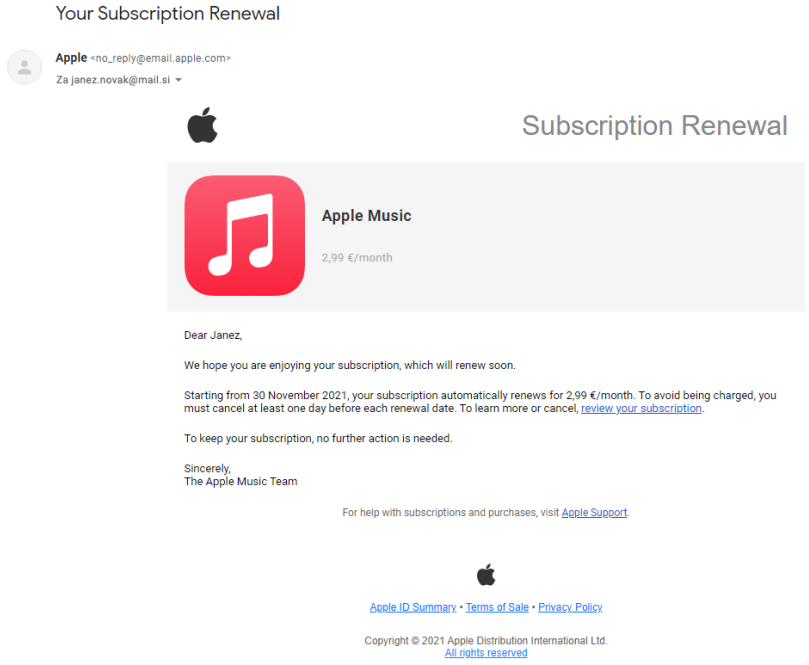

Figure 9: Apple Inc. (genuine).

Figure 10: Intesa Sanpaolo Bank (genuine).

Acknowledgements

We would like to thank the Dean, the Student Council and the Student Office of the Faculty of Criminal Justice and Security at the University of Maribor for showing and providing supporting during our study. We also thank all participants in the study for their eager participation and understanding.

References

[Abroshan et al., 2021] Abroshan, H., Devos, J., Poels, G., and Laermans, E. (2021). Covid-19 and Phishing: Effects of Human Emotions, Behavior, and Demographics on the Success of Phishing Attempts During the Pandemic. *IEEE Access*, 9:121916–121929.

[Adebowale, 2021] Adebowale, M. A. (2021). Intelligent Decision Support System. In Soofastaei, A., editor, *Virtual Assistant*. IntechOpen.

[Alabdan, 2020] Alabdan, R. (2020). Phishing Attacks Survey: Types, Vectors, and Technical Approaches. *Future Internet*, 12(10):168.

[Alanezi, 2021] Alanezi, M. (2021). Phishing Detection Methods: A Review. *Technium: Romanian Journal of Applied Sciences and Technology*, 3(9):19–35.

[Alawida et al., 2022] Alawida, M., Omolara, A. E., Abiodun, O. I., and Al-Rajab, M. (2022). A deeper look into cybersecurity issues in the wake of Covid-19: A survey. *Journal of King Saud University - Computer and Information Sciences*, 34(10):8176–8206.

[Alkhalil et al., 2021] Alkhalil, Z., Hewage, C., Nawaf, L., and Khan, I. (2021). Phishing Attacks: A Recent Comprehensive Study and a New Anatomy. *Frontiers in Computer Science*, 3:563060.

[Andress, 2019] Andress, J. (2019). *Foundations of information security: a straightforward introduction*. No Starch Press, San Francisco.

[Bayl-Smith et al., 2022] Bayl-Smith, P., Taib, R., Yu, K., and Wiggins, M. (2022). Response to a phishing attack: persuasion and protection motivation in an organizational context. *Information & Computer Security*, 30(1):63–78.

[Bullee et al., 2017] Bullee, J.-W., Montoya, L., Junger, M., and Hartel, P. (2017). Spear phishing in organisations explained. *Information & Computer Security*, 25(5):593–613.

[Butavicius et al., 2022] Butavicius, M., Taib, R., and Han, S. J. (2022). Why people keep falling for phishing scams: The effects of time pressure and deception cues on the detection of phishing emails. *Computers & Security*, 123:102937.

[CERT-EU, 2024] CERT-EU (2024). Threat Landscape Report 2023 - Year Review. Technical report, CERT-EU.

[Das et al., 2020] Das, A., Baki, S., El Aassal, A., Verma, R., and Dunbar, A. (2020). SoK: A Comprehensive Reexamination of Phishing Research From the Security Perspective. *IEEE Communications Surveys & Tutorials*, 22(1):671–708.

[Diaz et al., 2020] Diaz, A., Sherman, A. T., and Joshi, A. (2020). Phishing in an academic community: A study of user susceptibility and behavior. *Cryptologia*, 44(1):53–67.

[ENISA, 2023] ENISA (2023). ENISA Threat Landscape 2023. Technical report, ENISA.

[Fujs et al., 2021] Fujs, D., Vrhovec, S., and Vavpotic, D. (2021). Know Your Enemy: User Segmentation Based on Human Aspects of Information Security. *IEEE Access*, 9:157306–157315.

[Fujs et al., 2020] Fujs, D., Vrhovec, S., and Vavpotič, D. (2020). Bibliometric Mapping of Research on User Training for Secure Use of Information Systems. *Journal of Universal Computer Science*, 26(7):764–782.

[Fujs et al., 2022] Fujs, D., Vrhovec, S., and Vavpotič, D. (2022). Towards Personalized User Training for Secure Use of Information Systems. *The International Arab Journal of Information Technology*, 19(3).

[Ghazi-Tehrani and Pontell, 2021] Ghazi-Tehrani, A. K. and Pontell, H. N. (2021). Phishing Evolves: Analyzing the Enduring Cybercrime. *Victims & Offenders*, 16(3):316–342.

[Gordon et al., 2019] Gordon, W. J., Wright, A., Aiyagari, R., Corbo, L., Glynn, R. J., Kadakia, J., Kufahl, J., Mazzone, C., Noga, J., Parkulo, M., Sanford, B., Scheib, P., and Landman, A. B. (2019). Assessment of employee susceptibility to phishing attacks at us health care institutions. *JAMA Network Open*, 2(3):e190393.

[Hassandoust et al., 2020] Hassandoust, F., Singh, H., and Williams, J. (2020). The role of contextualization in individuals' vulnerability to phishing attempts. *Australasian Journal of Information Systems*, 24.

[Heartfield and Loukas, 2016] Heartfield, R. and Loukas, G. (2016). A Taxonomy of Attacks and a Survey of Defence Mechanisms for Semantic Social Engineering Attacks. *ACM Computing Surveys*, 48(3):1–39.

[Iuga et al., 2016] Iuga, C., Nurse, J. R. C., and Erola, A. (2016). Baiting the hook: factors impacting susceptibility to phishing attacks. *Human-centric Computing and Information Sciences*, 6(1):8.

[Jampen et al., 2020] Jampen, D., Gür, G., Sutter, T., and Tellenbach, B. (2020). Don't click: towards an effective anti-phishing training. A comparative literature review. *Human-centric Computing and Information Sciences*, 10(1):33.

[Lain et al., 2022] Lain, D., Kostiainen, K., and Capkun, S. (2022). Phishing in Organizations: Findings from a Large-Scale and Long-Term Study. In *2022 IEEE Symposium on Security and Privacy (SP)*, pages 842–859, San Francisco, CA, USA. IEEE.

[Lappas and Karampelas, 2023] Lappas, D. and Karampelas, P. (2023). Designing an Email Attack by Analysing the Victim's Profile. An Alternative Anti-Phishing Training Method. In *European Conference on Cyber Warfare and Security*, pages 257–266.

[Lee et al., 2023] Lee, Y. Y., Gan, C. L., and Liew, T. W. (2023). Thwarting Instant Messaging Phishing Attacks: The Role of Self-Efficacy and the Mediating Effect of Attitude towards Online Sharing of Personal Information. *International Journal of Environmental Research and Public Health*, 20(4):3514.

[Mihelič et al., 2019] Mihelič, A., Jevšček, M., Vrhovec, S., and Bernik, I. (2019). Testing the human backdoor: Organizational response to a phishing campaign. *Journal of Universal Computer Science*, 25(11):1458–1477.

[Mughaid et al., 2022] Mughaid, A., AlZu'bi, S., Hnaif, A., Taamneh, S., Alnajjar, A., and Elsoud, E. A. (2022). An intelligent cyber security phishing detection system using deep learning techniques. *Cluster Computing*, 25(6):3819–3828.

[Nasser et al., 2020] Nasser, G., Morrison, B. W., Bayl-Smith, P., Taib, R., Gayed, M., and Wiggins, M. W. (2020). The Role of Cue Utilization and Cognitive Load in the Recognition of Phishing Emails. *Frontiers in Big Data*, 3:546860.

[Parmar, 2012] Parmar, B. (2012). Protecting against spear-phishing. *Computer Fraud & Security*, 2012(1):8–11.

[Parsons et al., 2017] Parsons, K., Calic, D., Pattinson, M., Butavicius, M., McCormac, A., and Zwaans, T. (2017). The Human Aspects of Information Security Questionnaire (HAIS-Q): Two further validation studies. *Computers & Security*, 66:40–51.

[Patil and Arra, 2022] Patil, K. and Arra, S. R. (2022). Detection of Phishing and User Awareness Training in Information Security: A Systematic Literature Review. In *2022 2nd International Conference on Innovative Practices in Technology and Management (ICIPTM)*, pages 780–786, Gautam Buddha Nagar, India. IEEE.

[Sharma et al., 2022] Sharma, P., Dash, B., and Ansari, M. F. (2022). Anti-Phishing Techniques – A Review of Cyber Defense Mechanisms. *International Journal of Advanced Research in Computer and Communication Engineering*, 11(7).

[SI-CERT, 2023] SI-CERT (2023). Poročilo o kibernetski varnosti za 2022. Technical report, SI-CERT.

[SlashNext, 2023] SlashNext (2023). The State of Phishing 2023. Technical report, SlashNext.

[Sutter et al., 2022] Sutter, T., Bozkir, A. S., Gehring, B., and Berlich, P. (2022). Avoiding the Hook: Influential Factors of Phishing Awareness Training on Click-Rates and a Data-Driven Approach to Predict Email Difficulty Perception. *IEEE Access*, 10:100540–100565.

[Tultul et al., 2022] Tultul, A. N., Afroz, R., and Hossain, M. A. (2022). Comparison of the efficiency of machine learning algorithms for phishing detection from uniform resource locator. *Indonesian Journal of Electrical Engineering and Computer Science*, 28(3):1640–1648.

[Williams et al., 2023] Williams, R., Morrison, B. W., Wiggins, M. W., and Bayl-Smith, P. (2023). The role of conscientiousness and cue utilisation in the detection of phishing emails in controlled and naturalistic settings. *Behaviour & Information Technology*, pages 1–17.

[Yoro et al., 2023] Yoro, R. E., Aghware, F. O., Malasowe, B. O., Nwankwo, O., and Ojugo, A. A. (2023). Assessing contributor features to phishing susceptibility amongst students of petroleum resources varsity in Nigeria. *International Journal of Electrical and Computer Engineering*, 13(2):1922.

[Zheng et al., 2022] Zheng, F., Yan, Q., Leung, V. C., Richard Yu, F., and Ming, Z. (2022). HDP-CNN: Highway deep pyramid convolution neural network combining word-level and character-level representations for phishing website detection. *Computers & Security*, 114:102584.